

# IT Security Audit



## Beschreibung

Die Informatik ist immer stärker verantwortlich für das Erstellen und die Abwicklung von geschäftskritischen Abläufen und wird dadurch zum unmittelbaren Erfolgsfaktor eines Unternehmens. Durch den Einsatz dieser Betriebsmittel und die Tatsache, dass Computerprogramme immer wieder fehlerhaft sind oder ungenügend konfiguriert werden, setzt sich das Unternehmen einem Risiko aus, das es zu beurteilen gilt.

Zusätzlich bestehen in vielen Branchen regulatorische oder gesetzliche Vorgaben, die den Aufbau und den Betrieb von IT-Anwendungen vorgeben und die regelmässig überprüft werden müssen.

## Kundennutzen

Mit der Durchführung eines IT Security Audits setzen Sie sich proaktiv mit dem Thema auseinander und erarbeiten eine Entscheidungsgrundlage für das Risikomanagement des gesamten Unternehmens. Sie wissen, welche Abhängigkeiten zu internen und externen IT-Partnern bestehen, welche Informationen es zu schützen gilt, wo Sie besonders verletzlich sind und welche Massnahmen zur Verbesserung ergriffen werden können.

## Leistungsumfang

Um den Umfang eines solchen IT-Security-Audit-Projektes bestimmen zu können, werden der Untersuchungsgegenstand, die Sicht und die Untersuchungstiefe gemäss den Vorgaben oder der Empfehlung von terreActive festgelegt.



## Untersuchungsgegenstand

---

Zuerst wird der Umfang der Untersuchung von Organisation und Infrastruktur festgelegt. Es werden die folgenden Themen berücksichtigt:

Organisation:

- Policies
- Prozesse
- sonstige Dokumente (Inventare, Pläne, Konzepte etc.)

Technik:

- physische Sicherheit
- Netzwerksicherheit
- Systemsicherheit
- Applikationssicherheit

## Sicht

---

Die IT einer Organisation stellt sich von innen und von aussen gesehen völlig unterschiedlich dar. Während beispielsweise bei der internen Sicht die Verfügbarkeit von Fileservern oder die Vertraulichkeit von Buchhaltungsdaten eine zentrale Rolle spielen, sind bei der Sicht von aussen etwa die Unangreifbarkeit des Webauftritts oder die Undurchdringlichkeit der Schnittstellen zwischen Internet und Intranet wesentlich.

Bei der Frage, welche Sicht das Audit berücksichtigen soll, ist zu bedenken, dass der weitest-  
aus grösste Schaden den Unternehmen durch Insider zugefügt wird.

## Untersuchungstiefe

---

Die gewünschte Untersuchungstiefe bestimmt, mit welchen Werkzeugen und Methoden und bis zu welchem Punkt die Untersuchungen betrieben werden. Zwei Begriffe, die häufig in Zusammenhang mit IT Security Audits zu hören sind, lauten «Black Box Testing» und «White Box Testing». Beim Black Box-Ansatz hat der Auditor keinen Zugang zu internen Informationen des Kunden und befindet sich somit in der Rolle eines (internen oder externen) Hackers. Demgegenüber steht der White Box-Ansatz, bei dem im Rahmen des Audits der Auditor beispielsweise Gespräche mit (Sicherheits-)Verantwortlichen führt oder Zugang zu interner Dokumentation hat.

Die von uns verfolgte Methodik ist grundsätzlich das White Box Testing. Ein Black Box Audit birgt stets die Gefahr eines falschen positiven Resultats und bringt daher dem Kunden den geringeren Nutzen.



Der Aufwand bei einem IT Security Audit bemisst sich grob nach der Formel **Breite x Tiefe**. Wenn also das Untersuchungsobjekt nicht eingegrenzt ist, ist es für den Kunden oftmals vorteilhaft, mit einem breit angelegten Assessment zu beginnen. Darauf aufbauend kann eine intensivere Auseinandersetzung mit spezifizierten Bereichen der IT-Infrastruktur folgen, beispielsweise ein Audit des internen Netzwerks oder ein Penetration-Test des Internetauftritts.

Unser Angebot gliedert sich nach der vom Kunden gewünschten Untersuchungstiefe:

**Assessment**  
(siehe Abb. 1)

Das Assessment ist die oberste, am wenigsten intensive Stufe eines IT Security Audits. Im Zentrum des Assessments steht die Bestandsaufnahme der sicherheitsrelevanten IT-Komponenten eines Unternehmens.

Die zentrale Aufgabe eines Assessments ist es jedoch, sowohl dem Kunden als auch terreActive einen Überblick über die Sicherheitskomponenten zu verschaffen und herauszufinden, an welchen Stellen der Handlungsbedarf am grössten ist.

**Examination**  
(siehe Abb. 2)

Die Examination ist die mittlere Stufe eines IT Security Audits, wobei die Untersuchung weiter eindringt als ein Assessment, ohne jedoch die Tiefe eines Penetration-Tests zu erreichen. Im Gegensatz zu einem Assessment ist bei einer Examination der Untersuchungsgegenstand klar festgelegt und dokumentiert. Im Allgemeinen wird nicht die gesamte IT-Infrastruktur eines Unternehmens einer Examination unterzogen, vielmehr beschränkt sich die Prüfung auf einen beispielsweise funktional (Webhosting-Infrastruktur), räumlich (IT-Infrastruktur am Standort X) oder technologisch (Unix-Datei- und -Applikationsserver) abgegrenzten Teilbereich. Im Rahmen der Examination werden alle organisatorischen und technischen Komponenten des zu untersuchenden Bereichs unter die Lupe genommen.

**Penetration-Test**  
(siehe Abb. 3)

Bei dieser Form des Audits stehen keine internen Informationen über die IT-Infrastruktur zur Verfügung, das heisst, der Auditor befindet sich in der Rolle des anonymen Angreifers (Hacker), um einen möglichst realen Angriff zu simulieren. Damit werden bekannte Sicherheitslücken aufgedeckt, die zu Problemen führen können und so direkte Bedrohungen darstellen.

Falls Sie eine unabhängige Zweitmeinung zum Thema IT-Sicherheit wünschen, offerieren wir Ihnen zusätzlich ein Audit in Form einer 2nd Opinion (siehe Rückseite).



### Die drei Audit-Stufen in Kürze:

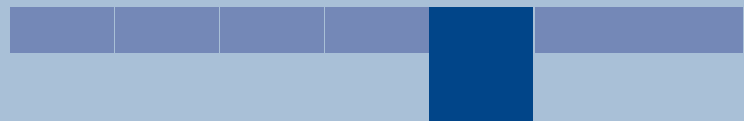
#### Assessment (Abb. 1)

Hier handelt es sich um eine in die **Breite** angelegte Untersuchung sämtlicher sicherheitsrelevanter IT-Komponenten, die einen Überblick darüber vermittelt, wo der Bedarf nach einer tieferen Untersuchung am grössten ist.



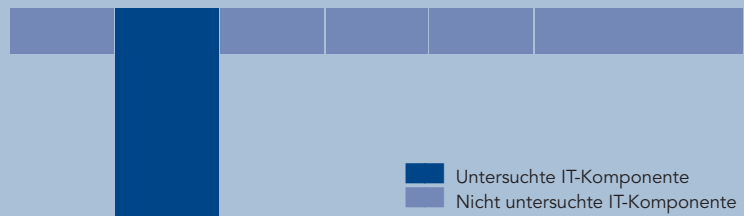
#### Examination (Abb. 2)

Ein ausgewählter Teilbereich Ihrer IT-Komponenten wird vertieft untersucht und dokumentiert. Die Untersuchung dringt tiefer ein als beim Assessment, aber weniger tief als beim Penetration-Test.



#### Penetration-Test (Abb. 3)

Das Untersuchungsobjekt ist bei dieser Form des Audits am stärksten eingegrenzt und erfährt die intensivste Auseinandersetzung, das heisst, die Untersuchung geht am meisten in die **Tiefe**.



Die drei Audit-Stufen können alle hintereinander oder auch jede für sich alleine durchgeführt werden. Die zu untersuchenden IT-Komponenten sowie die Untersuchungstiefe können Sie frei wählen.



## 2nd Opinion

Durch eine 2nd Opinion erhalten Sie die Gewissheit, dass das Re-design Ihrer Sicherheitsarchitektur auf dem richtigen Weg ist. Machbarkeit und eventuelle, verdeckte Kosten werden aufgezeigt, sodass Sie Änderungen oder Verbesserungen vornehmen können, bevor die eigentliche Implementierungsphase angefangen hat. Zudem erhalten Sie eine Analyse Ihrer operativen Prozesse, die Ihnen hilft, die nötigen Schritte einzuleiten, um die Sicherheitsarchitektur betreiben zu können. Sie können sich bei Ihren Entscheidungen auf eine zweite Meinung verlassen. Weiter können mögliche Fehler sehr früh erkannt und vermieden werden, was sich positiv auf die Gesamtprojektkosten auswirkt.

## Projektablauf

---

Die Durchführung eines IT Security Audits läuft in folgenden Phasen ab:

### Phase Inhalt

1	Kick-off-Meeting /Administration
2	Informationsbeschaffung
3	Zwischenbericht/-besprechung
4	Detailanalyse
5	Abschlussbericht/-präsentation

## Resultate

---

Als Ergebnis erhalten Sie eine Präsentation und einen ausführlichen Bericht mit folgendem, der Art des Audits entsprechendem Inhalt:

- Soll/Ist-Vergleich der vorgefundenen Organisation
- Stärken/Schwächen-Analyse (Risikobeurteilung)
- Massnahmenkatalog zur Behebung der vorgefundenen Schwächen
- Inventardokumente

Der Bericht ist so gegliedert, dass er für verschiedene Zielgruppen verwendet werden kann. Im Management Summary finden Sie eine Zusammenfassung der Bedrohungen und der Massnahmen, die anschliessenden Kapitel listen die untersuchten Objekte sowie die gefundenen Stärken und Schwächen mit einer Risikoanalyse und empfohlenen Massnahmen auf. Im Anhang befinden sich alle Informationen, die während der Untersuchung festgehalten wurden und als Grundlage für die Analyse dienen.

Die Abschlusspräsentation wird entsprechend dem Publikum aus dem Bericht extrahiert, sodass der Inhalt abgestimmt ist.

## Kontakt

---

Gerne erarbeiten wir Ihnen ein detailliertes Angebot. Kontaktieren Sie uns:

Kasinostrasse 30, CH-5001 Aarau  
Tel.: 062 823 93 55, Fax: 062 823 93 56  
[www.terreActive.ch](http://www.terreActive.ch), [info@terreActive.ch](mailto:info@terreActive.ch)

© terreActive AG

Die – auch auszugsweise – Reproduktion, Übersetzung  
sowie sonstige Verwendung der Inhalte dieser  
Publikation ist nur nach ausdrücklicher Genehmigung  
durch terreActive AG gestattet. Änderungen vorbehalten.



**Wir sichern Ihren Erfolg.**

terre**Active**  
terre**Active**  
terre**Active**  
terre**Active**